AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

OPERATIONAL RESILIENCE FOR 2040

by

Peter C. Mastro, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Jason M. Trew

Maxwell Air Force Base, Alabama

April 2014

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

The proliferation of advanced capabilities, the increasing complexity of the operational environment, and the enduring nature of surprise in warfare will combine by 2040 to fundamentally change the way the United States projects military power. No longer will it rely on sanctuary, from both distance and technological means, to create an optimized force for an environment it controls. In 2040 the United States will need to be prepared to fight in a complex and contested environment characterized by change, disruptions, and surprise. To succeed in that environment it will need to maintain its core purpose and integrity in the face of dramatically changed circumstances or disruptions; it will need to be resilient. This transformation will require technology solutions that reduce system vulnerabilities through redundancy, diversity, disaggregation, and the introduction of slack. In addition, technology and methods are needed to increase system adaptability through increased sensing of the environment, means to make decisions through disruptions, and change through scalability and modifiability. This paper provides technology examples that will contribute to this transformation to maintain a force that can confidently provide military options to the President of the United States in 2040.

Contents

Tables

Introduction

The United States has achieved remarkable military capabilities across the range of military operations, from speed and lethality during major combat operations to global reach, presence, and situational awareness for contingencies. However counterintuitively, many of the capability increases have caused a corresponding increase in vulnerabilities. Potential adversaries increasingly recognize they can significantly reduce United States military capabilities if they disrupt a few key vulnerabilities. Fortunately, this is also recognized by the United States military. The Capstone Concept for Joint Operations in 2020 recognizes the proliferation of advanced weapons to adversaries who may seek to exploit U.S. vulnerabilities in asymmetric ways is one contributing factor that will create an unpredictable, complex, and dangerous environment.[1] The United States has created a force that is very capable given its uninhibited access to systems across all domains (air, cyber, land, maritime, and space) while its capabilities are disproportionately curtailed if this access is disrupted. In this way the United States military's operational architecture is fragile. The operational environment of 2040 requires the United States to develop a military that is resilient to disruption and surprise. This paper will explain why resiliency is necessary and will describe its enabling attributes. Lastly, this paper will provide technology examples the U.S. military can pursue to make the resilient force of 2040 a reality.

A Fragile Operational Architecture

The operational architecture is the collection of military assets, communications means, and resource links between military assets. It is fragile when it has decreased effectiveness of its core purpose and integrity in the face of dramatically changed circumstances or disruptions. A fragile architecture will break disproportionately with non-linear negative effects when exposed to a particular disruption. For example, if doubling a disruption's intensity results in greater than twice the damage to the system it is considered fragile to that disruption.[2] This is consistent with the common understanding of fragility. A china tea cup, typically considered fragile, can withstand a tap on its side from a knife, even many successive taps, without any noticeable damage. However, doubling the tap's intensity could cause the tea cup to break, resulting in a catastrophic failure in its ability to perform its function. This catastrophic failure is disproportionally greater than a mere doubling of the damage done to the cup by the initial taps (i.e. it is not simply additive).[3] This is analogous to the U.S. military that can withstand and defend against certain disruptions while other disruptions focused on vulnerable leverage points can cause catastrophic degradation of capability. The United States military has increased the fragility of its operational architecture through two main processes. First, when upgrading capabilities it has repeatedly been willing to accept more vulnerable dependencies in exchange for remarkably more capable systems. Secondly, it has pursued operational efficiencies while attempting to maximizing effectiveness.

Most current military systems depend on specialized resource inputs to perform their function compared to previous less capable versions of the system. This specialization requires standardized inputs to come from fewer sources and increases the time to regenerate the input if disrupted. These changes increase the input's vulnerability and decrease the system's ability to adapt if the needed input is no longer available. The Joint Chiefs of Staff Concept on Joint Operations 2020 explains, "Standardization may lead to decreased diversity, flexibility, versatility and, ultimately effectiveness".[4] For example, during the 20th century, methods of navigation transitioned from the magnetic field of the Earth, position of the stars, and sun to radio waves emanating from satellites on orbit. This change in navigation methods significantly increased capability while the number of sources of navigation information decreased, additional systems were required to generate and interpret specialized signals, and links became more vulnerable to attack. Acceptance of increased vulnerability in exchange for increased capability spans across the entire force. In fact, this has been continuing for millennia. The first people to abandon the stick as a weapon in favor of a forged metal weapon were making the choice to increase their capability while accepting decreased weapon sources that were easier for the enemy to disrupt.

The United States military has also increased its fragility by focusing on system design approaches that seek efficiencies while attempting to maximize effectiveness. Approaches such as operational research, systems analysis, and systems engineering, referred to as "hard systems thinking," seek to optimize the performance of a system in pursuit of clearly identified goals for an assumed future environment.[5] Several methods are used to optimize a system. For example, system designers remove assets and processes that are not perceived to contribute to delivering the desired end-state. They standardize functions, inputs, and outputs to facilitate the internal integration and smooth functioning of the system processes and they consolidate functional division to allow greater control over how each function is performed. The resulting system excels at delivering the desired capability for the least cost. However, if the environment in which the system is operating changes or if operators find they require different capabilities the system may have no ability to adapt. These system approaches struggle with significant complexity and with multiple possible end-states.[6] Different approaches are needed to ensure the operational architecture can remain viable in complex and turbulent environments.[7]

These changes have made the United States military more susceptible to operational failure from disruption and surprise and require greater resources committed to protecting system vulnerabilities. Removing assets from the operational architecture increases the importance each remaining asset has on the functioning of the system. The loss of one B-2 out of the total 21 produced certainly degrades the U.S. total bombing capability more than losing one B-17 during World War II out of the over 12,000 produced.[8] In order to successfully rely on so few but capable assets, protection of each asset has to be of greatest importance. Secondly, standardization of process spreads common vulnerabilities across the military force. This is seen in the F-35 that will be used by the US Air Force, Navy, and Marines as well as ten other countries.[9] As just one example, if a future adversary identifies a vulnerability to exploit in the F-35 they could potentially degrade the capability of the United States and its allies to a larger degree and with less effort than if these militaries used many different airplanes. As the operational architecture becomes more fragile, more knowledge is needed about threats in order to protect against disruptions. This increases resources committed toward acquiring threat knowledge and specific defense mechanisms.[10,11] Ironically, the expectation to suppress volatility through knowledge and protection in turn further increases fragility.[12] This is because the contributors to fragility flourish behind the walls of protection where it is believed the enemy cannot take advantage of the growing vulnerabilities. Unfortunately, expecting to suppress volatility, eliminate surprises, and protect assets in the future operational environment is increasingly a losing proposition.

The Future Environment

The United States should expect a less permissive operational environment in 2040 with increased disruptions and changing circumstances during combat operations. The less permissive environment is caused by the dramatic improvement and proliferation of technology capable of denying access or freedom of action within an operational area, referred to as anti-access/area denial (A2/AD) capabilities.[13,14] These capabilities include the proliferation of precise long-range missiles, anti-space capabilities, and cyber weapons. The Department of Defense's Capstone Concept for how the Joint Force will operate in the future describes an environment that is "likely to be more unpredictable, complex, and potentially dangerous than today."[15] The combination of long range weapons with greater accuracy is driving this change.

In addition to a less permissive environment, the future battlefield will continue to include uncertainty and surprise, as it always has. This does not require a technologically advanced adversary, only a thinking adversary dedicated to using their strengths to counter the perceived weaknesses of the U.S. military. Examples of surprise date back to war's earliest recordings at the battle of Megiddo when the Egyptian Pharaoh Thutmose III led his forces through the Musmus Pass catching the defenders at Megiddo off guard.[16] Uncertainty and surprise will remain inherent in the nature of competition between creative humans dedicated to accomplishing their goals against an adversary.[17] The combination of the enduring nature of surprise and increased adversary capability calls into question the United States military's ability to create sanctuaries to protect critical vulnerabilities; a current necessary condition for it to maintain a capability edge over its adversaries. These changes require the United States to develop a military that can operate through disruption and even thrive in it.

A Resilient Operational Architecture

Resilient operational architectures are needed to survive disruptions and surprises. Resiliency is the capacity of a system to maintain its core purpose and integrity in the face of dramatically changed circumstances or disruptions.[18] Resilient systems reduce the magnitude of damage done by disruptions and fail gracefully; this is in contrast to fragile systems where small disruptions can cause system failure.[19] Resiliency does not require maintaining the original structure of the system, in actuality, attempting to do so could be detrimental to the long-term viability of the system. Resiliency is similar to survivability that has been a requirement for military system for many years.[20] They both have similar contributing attributes and each aim to maintain functionality in a contested environment. However, survivability emphasizes individual platforms remaining robust or impervious to disruption while resiliency emphasizes the architecture or system of systems continuing to deliver military capability through system adaption.[21,22] By placing emphasis at a higher system of systems level, new ways to maintain functionality through disruption can be implemented. For example, resiliency allows some platforms to accept high risk of destruction to divert adversary resources while the rest of the system of systems continues to function against the enemy’s exposed vulnerabilities.

In any competition, only measuring one side’s capabilities, strengths, and weaknesses is less important than a relative comparison of these qualities against an adversary. Resiliency reduces system degradation due to disruptions and changes while providing a means to capitalize on changing circumstances. Therefore, if one force’s resiliency is greater than another’s, its relative effectiveness over an adversary increases as more changes and disruptions occur for both sides. This force will achieve an “antifragile” response in relative effectiveness. Antifragile, a term coined by Nassim Taleb, is defined as something that benefits from shocks, volatility, randomness, disorder, and stressors.[23] The antifragile response ensures there will be more upside (increased relative effectiveness) than down-side as disruptions occur.[24] Consequentially, when evaluating the U.S military’s capabilities, relative resiliency compared to potential adversaries must be a key qualitative measure. It is possible the United States military's perceived quality advantage over potential adversaries is reduced if resiliency is the measure of quality.

Resiliency Objectives

Military leaders constructing future operational architectures can use a number of attributes to increase three resiliency objectives of reducing susceptibility to disruption, reducing vulnerability to disruption, and increasing adaptability.[25] Susceptibility to disruptions is whether a threat will ever actually engage the system. Attributes that reduce susceptibility include increased mobility, avoiding threat areas, concealment, deception, dispersion of assets, and active defense.[26] The current operational architecture pursues these attributes and should continue to do so. However, the U.S. military cannot solely rely on them in the operational environment of 2040. This results in the requirement to place more attention on the next two resiliency objectives.

Reduced vulnerability to disruption reduces the impact to system functionality if disruptions do occur.[27] Attributes that reduce vulnerability include redundancy, diversity, disaggregation, and slack in system response.[28] Together these attributes can give the system the ability to absorb an attack and possibly deceive the attacker into thinking the system has been damaged when in fact it remains capable and ready to respond.[29] Redundancy is having multiple assets perform the same function or multiple sources of resource dependencies such as data or other physical resources.[30] Diversity refers to performing the same functions with different types of assets, data sources, or supply chains to limit vulnerability to any one specific failure mode. The diversity in system design should reflect the diversity of the environmental disturbances the system will have to operate through.[31] Disaggregation lowers the complexity of any particular asset while distributing the performance of a function over a group of assets.[32] Disaggregation uses dispersion and redundancy to increase the difficulty for adversaries to successfully target all assets that deliver a capability and increases their uncertainty of delivering a successful attack.[33] Slack reduces the coupling of system components and thereby loosens the ties between a disruption and the effect on the system.[34] It prevents failure in one area from quickly propagating to cause failures in other areas of the system. Slack provides time for the system to operate through and make sense of the new situation to allow the operator to take action prior to system failure.[35]

Resiliency's third objective is adaptability which is the ability to change in response to the environment. Attributes that increase adaptability include the ability to monitor the environment, determine when change is needed, and change through scalability and modifiability. Scalability is a change in the level of a particular parameter. For example, the ability to increase the number of assets delivering weapons on target. Modifiability is a change in the parameter set provided by the system. For example, the ability to add a new type of sensor into the operational architecture in response to an emerging need.[36]

Table 1: Resiliency Objectives and Attributes

Resiliency Objectives	Resiliency Attributes
Reduce Susceptibility to Disruptions	Mobility Avoidance Concealment Deception Dispersion Active Defense
Reduce Vulnerability to Disruptions	Redundancy Diversity Disaggregation Slack
Increase Adaptability	Monitor Environment Determination of Change Scalability Modifiability

Technology Examples

Technology can play an important role in developing solutions to achieve resiliency objectives. The problem technology must solve is how to enhance resiliency attributes while maintaining a highly capable and affordable force. The balance between increasing resiliency without forfeiting capability is important. It is not acceptable to simply give up a capability or domain because of its vulnerability. Therefore the risk from vulnerabilities needs to be weighed against the benefits and costs of resiliency. The remainder of this paper will provide suggestions on research areas, technology development, and examples of on-going projects that contribute to resiliency attributes that support reducing vulnerability and increasing adaptability. These examples are provided to clarify the resiliency attributes and are not an exhaustive list of necessary technology for a resilient military force.

Redundancy

The first attribute to highlight is redundancy, specifically, redundant platforms capable of performing the same function. The U.S. Military of 2040 should have a greater quantity of individual assets with increased capability at the system of systems level combating the current trend toward fewer highly capable assets. Using many lower cost assets to perform offensive and defensive functions can be implemented as swarming. Swarming uses dispersion, mobility, and redundancy to cause targeting problems for the adversary.[37,38] This approach is gaining attention across the defense community. The United States Scientific Advisory Board has recommended "the Air Force can improve mission robustness in contested environments via increased platform redundancy. Enablers include low-cost design and airframe/engine/electronics…swarming…exploiting redundancy-based methods."[39]

Some have referred to this debate as "quantity versus quality," however this description is misleading. It assigns the term "quality" to the approach that attempts to have high capability at the platform level without regard to whether those platforms can survive in the future environment. Meanwhile, labeling the approach with greater quantity of individual assets simply "quantity" misses that this approach also has high capability and quality but it is held at the higher system of systems level, not at the platform level.

Swarming usually limits itself to those assets that perform direct offensive and defensive functions. However, the U.S. military needs to increase redundancy of all assets that perform a critical function. An example of this is DARPA's LANdroid program that aims to improve communications at the tactical level by distributing many inexpensive robotic radio-relays to reduce the vulnerability caused from few communication paths between tactical forces and higher command.[40] Redundancy needs to extend to other communication systems, resource distribution centers, command and control systems, and other critical functions.

In addition to redundancy of assets, redundancy of resource sources is also needed. Ideally, the military would identify each resource that is needed for an asset to perform its function (fuel, information, armaments, etc.) and maximize the number of ways the asset could receive that resource. This combats the trend of reducing the resource sources due to specialization. For example, a significant resource need of current systems is information. One technological solution is Wireless Mesh Networks already used in disaster response operations.[41] These provide a multiple-input multiple-output (MIMO) solution.[42] Other technologies and systems are in research, development, and initial operational use that increase this type of redundancy such as the Joint Aerial Layer Network (JALN) with the Battlefield Airborne Communications Node (BACN). [43] The platforms the U.S. military uses in 2040 should have multiple paths to receive the resources it needs to perform its function.

Of course, it is not difficult to argue that “more is better.” The difficulty is implementing redundancy at an acceptable cost. Redundancy as advocated in this paper will require significantly less expensive individual assets. This requires design trades to determine the capabilities of individual platforms (a key parameter for their cost per unit) and the capability delivered through the interaction of these assets at the higher system of systems or architecture level. Encouragingly, one of the seven DoD Science and Technology priority areas is “Engineering Resilient Systems.”[44] The tools generated through this initiative may prove helpful to perform these architecture level capability trades.[45] Sometimes the best way to increase the quantity of assets and resource sources is to increase the different types of assets and resources the system can use, also called diversity.

Diversity

Diversity is a special type of redundancy. Similar to redundancy, diversity aims to perform a function with multiple assets or rely on multiple sources of resources. However unlike redundancy, diversity purposefully performs these functions in different ways. Its aim, similar to redundancy, is to eliminate single point failures.[46] Diversity combats the previously identified tendency toward standardization. Valuing diversity requires respect for the uncertainty of future threats and acknowledging having multiple ways of doing things will minimize vulnerability and maximize ability to survive, even if no one can identify the specific threat in advance.

The value of performing a function in different ways is particularly beneficial when applied across domains since common failure modes are even less likely. For example, augmenting satellite communication or navigation services through capabilities in other domains makes the delivery of the capability more resilient from attack. Projects exist today to develop persistent near space communication relays. The Air Force recently released a Request For Information to industry searching for "Affordable Aerial Relays" to act as pseudo-satellites.[47,48] The 2040 military needs to significantly increase cross-domain functional diversity.

The military of 2040 also needs much more diversity in how it navigates. The widespread reliance on the Global Positioning System (GPS) has created a vulnerability that can be mitigated by adding another source of navigation information. For example, the DARPA Adaptable Navigation Office is exploring a highly accurate navigation system based on cold atom technology that will keep accurate navigation for much longer durations with fewer external position fixes.[49,50] DARPA is also developing navigation systems that use signals of opportunity in the environment such as signals from known radio, cell phone, and television towers to determine location.[51] This concept is particularly useful because it achieves diversity in function (how location is determined) and diversity in input (what is used to determine location) to compute the navigation solution. This may add additional vulnerabilities since these signals may be easier for the adversary to purposefully spoof. However, decision makers may find this risk acceptable if it is not the only source for navigation information, highlighting the benefit of diversity.

In 2040 the U.S. military needs the technology to transmit information in multiple ways. The Air Force has highlighted this need by stating in its technology vision that frequency agile capabilities are needed to ensure access to available spectrum bands.[52] A technology example is the use of phased array antennas that can receive signals over a broad range but also select a specific frequency for use.[53] In addition, research should be conducted for diversity in the ways platforms communicate without electromagnetic radiation such as through sound.

Lastly, the 2040 operational architecture needs energy diversification. The military should develop systems that can use alternate fuel sources and hybrid systems that can be powered using multiple means.[54] Fortunately the DoD has codified this goal in their operational energy strategy stating, “The Department needs to diversify its energy sources.”[55] A current example that could be promoted is the Navy’s Future Fuels Program in the Office of Naval Research.[56] Ultimately, research and development should aim to develop ways U.S. forces can obtain energy from their immediate surroundings relying on multiple sources that the adversary is unable to disrupt.

Disaggregation

The next attribute to highlight is disaggregation. This takes missions that are currently performed by singular platforms and breaks up the subcomponents onto multiple platforms working together to deliver the capability. In this sense disaggregation is dispersion applied to the subcomponent level. When redundancy is added to this subcomponent dispersion, disaggregation can result in very resilient architectures. An application of disaggregation in information processing is federated mission computing where computing is accomplished in multiple locations as opposed to centralized computing.[57]

Air Force Space Command (AFSPC) has placed great emphasis on disaggregation as a method to achieve resilient satellite constellations. The problem of operating a fragile architecture in a contested environment may be most acute in the space domain making it understandable that AFSPC is aggressively approaching the concept of resiliency and disaggregation. The AFSPC Commander has acknowledged satellite constellations must passively survive this environment and he identified disaggregation as a path to explore.[58] AFSPC explains that disaggregation improves mission survivability by increasing "the number and diversity" of targets for the enemy and complicating their decision calculus.[59] An example of an early enabler of this concept was the commercially hosted infrared payload (CHIRP) demonstration that placed a missile detection sensor aboard a commercial communication satellite.[60] Future efforts in all domains should look at possible ways to acceptably disaggregate missions.

Slack

The next attribute, slack, aims to increase the time between a disruption and wide scale system degradation. It is achieved by maintaining reserves of a resource above what is required for nominal operations. This allows operations to continue for some period of time if a dependency ceases to deliver the required resource. The U.S. military should review resource requirements to evaluate which exhibit the greatest risk to system degradation and provide appropriate margin to create slack. These reserves will not appear efficient in steady-state operations but may prove essential in a contested future environment. Therefore, decisions are necessary to determine the appropriate resources to maintain in reserve. One of the forces greatest requirements is fuel. Research and development is needed to increase energy efficiency and energy storage to maintain this reserve.[61,62] The military must look for ways to increase reserves as close to the point of operational use as possible.

Adaptability

To this point, technology to support reducing the vulnerability to disruption has been presented. Possibly more important is how the operational architecture can adapt to take advantage of new circumstances. Reducing the vulnerability and increasing adaptability are not independent from each other. Many of the attributes already listed are also features that make adaption possible.

Essential to adaption is determining who or what decides adaption is necessary and how it executes its decisions. Starting in the 1970s the work of Stafford Beer applied cybernetic concepts to organizational control; the result was the Viable System Model (VSM).[63] The VSM aims to describe the key features that any system must exhibit for it to sustainably manage complexity and turbulence.[64] While there are many aspects of the VSM, it is only necessary to highlight two fundamental ideas: ‘variety’ and ‘recursive nature’. Variety, based on the work of cybernetics pioneer Ross Ashby, is the number of states a system can exhibit. To ensure sustained operations, the total number of states a system’s operations can exhibit must be greater than or equal to the number of relevant states in its environment. Put another way, operations must have a way to deal with all the possible things that might happen from the environment. In addition, the variety of management that controls operations must be greater than or equal to the variety of operations.[65] Therefore, to create a sustainable system in a complex environment it is helpful to reduce the number of relevant states in the environment that can destroy a system; this is the purpose of the ‘reduce vulnerability’ resiliency objective. Meanwhile, system designers need to increase the variety of operations and control. VSM increases variety by leveraging the recursive nature of organizations. This means systems exist in hierarchies with organizational forms of higher levels repeating themselves in lower levels. [66] This self-similarity is also described as a fractal structure.[67] VSM aims to decentralize operations and control leaving lower levels as free as possible to deal with their environments.[68] This decreases the number of possible states each operational unit and control unit must exhibit while the total number of states the system can exhibit and control increases. These same principles are further advocated by military strategist John Boyd who stated, “Adaptability implies variety and rapidity. Without variety and rapidity one can neither be unpredictable nor cope with changing and unforeseen circumstances.”[69]

This is in essence the concept of Mission Command advocated by the Chairman of the Joint Chiefs of Staff, General Dempsey. The 2012 Whitepaper on Mission Command explains the necessity of this concept by first describing a complex, dynamic, and chaotic future environment where adversaries will challenge the United States through asymmetric means. Later it explains decentralization will, “provide us competitive adaptability and tempo advantages.”[70] Also fitting the VSM model is Mission Command’s focus on higher level command establishing intent and coordinating actions of subordinates while leaving the greatest amount of autonomy to lower units as possible. To identify the technology the U.S. military will required in 2040 it is best to look at the three Mission Command attributes of understanding, intent, and trust to highlight technology solutions that may assist with each.[71]

Understanding ensures decision-makers at all levels of the hierarchy have the proper insight and foresight to make decisions.[72] Using John Boyd's "OODA" model it is a combination of both observing the environment and orienting to shape observations and draw conclusions.[73] Focusing first on observation, the U.S. Military of 2040 will require increased monitoring of the military system and the operational environment to maximize adaptability. This requires leveraging the many dispersed assets across the operational environment and continuing the current emphasis that every platform and person is a sensor.[74] In addition, the operational architecture must removing obstacles to information sharing to increase decision makers' ability to gain a shared understanding.[75] One implementation is to ensure information is tagged and made available through cloud services.[76] The DoD Chief Information Officer recently published a Cloud Computing Strategy to increase information sharing and delivery.[77] Attention needs to be paid to ensure the drive for consolidating previously stove-piped IT systems does not increase systemic vulnerabilities. The use of commercial cloud services in what the CIO calls the multi-provider enterprise may be a means to mitigate this risk.[78]

Intent is a "clear and concise expression of the purpose of the operation and the desired military end state" and includes understanding, assigned missions, and direction to subordinates.[79] Mission command maximizes lower level initiative but still requires centralized control to ensure the coordinated action from the parts. The communication of intent is what binds the force together for coordinated action. However, if the command level that is issuing intent to subordinates is disrupted or destroyed the parts may not stay coordinated in their response to their environments as conditions change. In this scenario some level of coordination degradation may be inevitable; however, technology solutions may exist to offer some mitigation. Technological means are required in 2040 that can recognize when command and control is no longer possible from one entity and transfer command and control to another entity. For example, the Air Force controls theater air assets from the Air Operations Center (AOC) Weapon System. In 2040 technologies are required that can recognize when an AOC's operations have been disrupted and transfer control to other globally-distributed AOCs to continue providing Commander intent and coordination of forces.

Lastly, trust is what binds the force together and enables it to act as one.[80] There are multiple paths to develop trust across the force. One way for technology to support by 2040 is providing a richer training environment for decision makers. In fact, this training builds all aspects of mission command by increasing understanding, quick orientation, dissemination of intent, and building trust.[81] The mission command Whitepaper explains, "training should rehearse the Commander making rapid decisions without perfect or complete information. Training for mission command focuses the commander on gaining a comfort with uncertainty and chaos, and guided by intent, having the moral courage to decide quickly and act decisively."[82] While the proper mix between live training and training within a virtual environment must be balanced, the U.S. military should continue developing life-like and complex training in virtual environments that can expose operators to situations that may otherwise be restricted due to costs, physical reasons, or safety.[83] Programs like the Navy's Continuous Training Environment and the Army's integrated training environment should be expanded.[84]

Once a decision to adapt is made, the operational architecture needs the ability to support the change. Two forms of change are scalability and modifiability. Both methods require integrating new assets into the previously established operational architecture. In 2040, technology will need to continue to work toward open architectures with non-proprietary interfaces.[85] The 2040 military will have to do this while still maintaining diversity in functionality and dependencies. Multiple interface specifications can be used to allow designers multiple implementations that will still interoperate. One way to achieve this is through "gateways" such as DARPA's Mobile Ad Hoc Interoperability network Gateway (MAINGATE) that provides interconnectivity between previously incompatible radios.[86]

Conclusion

The proliferation of advanced capabilities combined with the enduring nature of surprise in warfare will fundamentally change the way the United States projects military power. No longer will it rely on sanctuary, from both distance and technological means, to create a highly efficient and optimized force for an environment it controls. In 2040 the United States will need to be prepared to fight in a complex and contested environment characterized by change, disruptions, and surprise. To succeed in that environment a force must be resilient to operate through disruption. This transformation will require modifications across the military force. This paper highlighted a few technology solutions that will contribute to this transformation to maintain a force that can confidently provide military options to the President of the United States in 2040.

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. *Capstone Concept for Joint Operations*, 2-3.
2. Taleb, *Antifragile*, 276.
3. Ibid., 268.
4. *Capstone Concept for Joint Operations*, 15.
5. Jackson, *Systems Thinking*, 16.
6. Ibid., 16.
7. Ibid., 21-22.
8. USWarplens.net, "Boeing B-17 Flying Fortress."
9. Lockheed Martin, "F-35 Lighting II, Global Participation."
10. Demchak, *Wars of Disruption and Resilience*, 46-47.
11. Bruijne, "Resilience," 21.
12. Taleb, *Antifragile,* 5.

13. *Joint Operational Access Concept*, ii.
14. *Capstone Concept for Joint Operations*, 3.
15. Ibid., 2-3.
16. Cline, *The Battles of Armageddon*, 6-7.
17. *The Joint Operating Environment 2010*, 5.
18. Zolli, *Resilience*, 7.
19. Richards, “Multi-Attribute Tradespace Exploration,” 61.
20. Ibid., 61.
21. Lindemuth, “Engineering Framework for Achieving Resiliency,” 6.
22. Richards, “Multi-Attribute Tradespace Exploration,” 51.
23. Taleb, *Antifragile*, 3.
24. Ibid., 5.
25. Richards, “Multi-Attribute Tradespace Exploration,” 88.
26. Ibid., 88.
27. Ibid., 61.
28. Ibid., 89.
29. Arquilla, *Networks and Netwars*, 13.
30. Demchak, *Wars of Disruption and Resilience*, 74.
31. Richards, “Multi-Attribute Tradespace Exploration,” 231.
32. Shelton, “Air Force Association Space Group Forum.”
33. *Resiliency and Disaggregated Space Architectures*, 2-3.
34. Demchak, *Wars of Disruption and Resilience*, 48.
35. Ibid., 74.
36. Ross and Hastings, *Assessing Changeability in Aerospace Systems*, 3.
37. Arquilla and Ronfeld, *Networks and Netwars*, 12.
38. Edwards, *Swarming on the Battlefield*, 81.
39. *Operating Next-Generation Remotely Piloted Aircraft*, 57.
40. McClure et al., “DARPA LANdroids Program,” Abstract.
41. Lussier, “Global Strike 2035,” 16.
42. *Unmanned Systems Integrated Roadmap*, 52.
43. Seffers, “Joint Aerial Layer Network.”
44. Department of Defense, “Department of Defense Research and Engineering Enterprise.”
45. Holland, “Engineered Resilient Systems.”
46. Richards, “Multi-Attribute Tradespace Exploration,” 74.
47. Office of the US Air Force Chief Scientist, *Technology Horizons*, 80.
48. Air Force Association, “Wanted, Satellite with Wings.”
49. Suriano, “Robust Technology to Augment or Replace,” 4.
50. DARPA, “DARPA Strategic Technology Office.”
51. Ibid.
52. Office of the US Air Force Chief Scientist, *Technology Horizons*, 75.
53. *Unmanned Systems Integrated Roadmap*, 47.
54. *Capstone Concept for Joint Operations*, 13.
55. Department of Defense, “Energy for the Warfighter,” 1.
56. Office of Naval Research, “Future Naval Fuels Program.”
57. *Unmanned Systems Integrated Roadmap*, 38.
58. Shelton, “Air Force Association Space Group Forum.”
59. *Resiliency and Disaggregated Space Architectures*, 2-3.
60. Pawlikowski et al. “Space: Disruptive Challenges.” 42.
61. *Unmanned Systems Integrated Roadmap*, 62.
62. *Capstone Concept for Joint Operations*, 13.
63. Jackson, *Systems Thinking*, 85.
64. Ibid., 25,86.
65. Ibid., 88-89.
66. Ibid., 87.
67. Ibid., 12.

68. Ibid., 93.
69. Boyd, “Organic Design for Command and Control,” 4.
70. *Mission Command Whitepaper*, 3.
71. Ibid., 5.
72. Ibid., 5.
73. Boyd, “Organic Design for Command and Control,” 13.
74. Schanz, “ISR After Afghanistan.”
75. Alberts, *The Agility Advantage*, 495.
76. *Capstone Concept for Joint Operations*, 9.
77. Chief Information Officer, “Cloud Computing Strategy”, Forward.
78. Ibid., Forward.
79. *Mission Command Whitepaper*, 5.
80. Ibid., 6.
81. Ibid., 7.
82. Ibidl, 7.
83. Government Accountability Office, “Navy Training,” 3.
84. Ibid., 10.
85. *Unmanned Systems Integrated Roadmap*, 31.
86. DARPA, “Radio Gateway.”

Bibliography

Alberts, David S., *The Agility Advantage: A Survival Guide For Complex Enterprises and Endeavors.* Command and Control Research Program Publication Series. September 2011.

Air Force Association. "Wanted, Satellite with Wings." Air Force Magazine. http://www.airforcemag.com/DRArchive/Pages/2014/March%202014/March%2006%202014/Wanted,-Satellite-with-Wings.aspx 6 March 2014 (accessed 10 March 2014).

Air Force Instruction (AFI) 62-201. *System Survivability*, 25 July 1994.

Arquilla, John and David Ronfeldt. *Networks and Netwars*. Santa Monica, CA: National Defense Research Institute RAND, 2001.

Birkland, Thomas A. "Federal Disaster Policy: Learning, Priorities, and Prospects for Resilience." In *Designing Resilience: Preparing for Extreme Events*, edited by Louis K. Comfort, Arjen Boin, and Chris C. Demchak, 109. Pittsburg, PA: University of Pittsburg Press, 2010.

Boyd, John R. "Organic Design for Command and Control." Presentation, May 1987.

Bruijne, Mark de, Argen Boin, and Michel van Eeten. "Resilience: Exploring the Concept and its Meanings." In *Designing Resilience: Preparing for Extreme Events*, edited by Louis K. Comfort, Arjen Boin, and Chris C. Demchak, 21. Pittsburg, PA: University of Pittsburg Press, 2010.

Capstone Concept for Joint Operations: Joint Force 2020. Joint Chiefs of Staff, 10 September 2012.

Mission Command Whitepaper. Chairman of the Joint Chiefs of Staff. Washington, DC: 3 April 2012.

Chief Information Officer. "Cloud Computing Strategy." Department of Defense Report. Washington, DC: July 2012.

Cline, Eric C., *The Battles of Armageddon: Megiddo and the Jezreel Valley from the Bronze Age to the Nuclear Age*. Michigan: The University of Michigan Press, 2003.

DARPA. "DARPA Strategic Technology Office." http://www.darpa.mil/Our_Work/STO/Programs/Adaptable_Navigation_Systems_(ANS).aspx (accessed 2 February 2014).

DARPA. "Radio Gateway connects U.S and Allied Troops to a common mobile network." http://www.darpa.mil/NewsEvents/Releases/2013/12/12.aspx 12 December 2013 (accessed February 2014).

Demchak, Chris C. *Wars of Disruption and Resilience: Cybered conflict, Power and National Security*. Athens, GA: The University of Georgia Press, 2011.

Department of Defense. "Department of Defense Research and Engineering Enterprise." http://www.acq.osd.mil/chieftechnologist/mission/index.html (accessed 31 Jaunuary 2014).

Department of Defense. "Energy for the Warfighter: Operational Energy Strategy." Report. Washington, DC: May 2011.

Edwards, Sean J. A., *Swarming on the Battlefield: Past, Present, and Future*. Santa Monica, CA: RAND, 2000.

Global Security. "Military Steam Propulsion." http://www.globalsecurity.org/military/systems/ship/steam3.htm (accessed 25 February 2014)

Government Accountability Office. "Navy Training: Observations on the Navy's Use of Live and Simulated Training." US Government Report GAO-12-725R. Washington, DC: 29 June 2012.

Holland, Jeffery P., "Engineered Resilient Systems (ERS)." Presentation, DoD Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), December 2013.

Jackson, Michael C., *Systems Thinking: Creative Holism for Managers*. West Sussex, England: John Wiley & Sons Ltd., 2003.

Joint Operational Access Concept, Version 1.0. Department of Defense, 17 January 2012.

The Joint Operating Environment 2010. Joint Forces Command, 18 February 2010.

Lindenmuth, Lt Col Steve, "Engineering Framework for Achieving Resiliency." Presentation. HQ AFSPC/A5X, 30 October 2013.

Lockheed Martin. "F-35 Lighting II, Global Participation: The Centerpiece of 21st Global Security." https://www.f35.com/global (accessed 5 April 2014).

Lussier, John K., "Global Strike 2035: Considerations For Enabling Effective Command and Control." Research Report. Maxwell AFB, AL: Air War College, 2012.

McClure, Mark, Daniel R. Corbett, and Douglas W. Gage. "DARPA LANdroids Program." *SPIE Proceedings, Unmanned Systems Technology XI* 7332 (April 2009).

Office of Naval Research. "Future Naval Fuels Program." http://www.onr.navy.mil/en/Science-Technology/Departments/Code-33/All-Programs/332-naval-materials/Future-Naval-Fuels.aspx (accessed 16 March 2014).

Office of the US Air Force Chief Scientist. *Technology Horizons: A Vision for Air Force Science and Technology 2010-2030.* Maxwell AFB, AL: Air University Press, 2011.

Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare. Scientific Advisory Board Report, SAB-TR-10-03. Washington, DC: Department of Defense, April 2011.

Pawlikowski, Lt Gen Ellen, Doug Loverro, and Col Tom Cristler. "Space: Disruptive Challenges, New Opportunities, and New Strategies." *Strategic Studies Quarterly* (Spring 2012): 27-54.

Resiliency and Disaggregated Space Architectures. United States Air Force Space Command White Paper. Colorado Springs, CO: Department of the Air Force, 2013.

Richards, Matthew G. "Multi-Attribute Tradespace Exploration For Survivability." PhD diss., Massachusetts Institute of Technology, April 2009.

Ross, Adam M. and Daniel E. Hastings. *Assessing Changeability in Aerospace Systems Architecting and Design Using Dynamic Multi-Attribute Tradespace Exploration.*AIAA 2006-7255 Space 2006. San Jose, CA: American Institute of Aeronautics and Astronautics, Inc., 19-21 September 2006.

Schanz, Marc V. "ISR After Afghanistan." *Air Force Magazine*, January 2013. http://www.airforcemag.com/MagazineArchive/Pages/2013/January%202013/0113ISR.aspx (accessed April 2014).

Seffers, George I. "Joint Aerial Layer Network Vision Moves Towards Reality." *Signal Magazine Online*, 1 June 2013. http://www.afcea.org/content/?q=node/11123.

Shelton, Gen William L., Commander Air Force Space Command. Address. Air Force Association Mitchell Institute Friday Space Group Forum, Washington, DC, 7 February 2014.

Suriano, Mark A., "Robust Technology to Augment or Replace the US Reliance on the Global Positioning System." Research Report. Maxwell AFB, AL: Air War College, 16 February 2011.

Taleb, Nassim Nicholas. *Antifragile: Things that Gain from Disorder*. New York, NY: Random House, 2012.

Unmanned Systems Integrated Roadmap. Department of Defense Report 14-S-0553, Washington DC: October 2013.

USWarplens.net. "Boeing B-17 Flying Fortress." http://www.uswarplanes.net/b17.html (accessed February 2014)

Zolli, Andrew and Ann Marie Healy. *Resilience: Why Things Bounce Back*. New York, NY: Simon & Schuster, 2012.